AD-A095 656 HARVARD UNIV CAMBRIDGE MASS AIKEN COMPUTATION LAB F/G 12/1
THE COMPLEXITY OF PROVABLE PROPERTIES OF FIRST ORDER THEORIES,(U)
1980 S HOMER, J H REIF N00014-80-C-0647
UNCLASSIFIED TR-21-80 NL

1 OF 1
AD
A095 656

END
DATE
FILMED
3-81
DTIC

2

THE COMPLEXITY OF PROVABLE PROPERTIES OF FIRST ORDER THEORIES

BY

Steve Homer
John H. Reif

TR-21-80

1980

(6)

THE COMPLEXITY OF PROVABLE PROPERTIES OF FIRST ORDER THEORIES,

(10) Steve/Homer*
John H./Reif**

(12) 27

11) 1981

(14) TR-22-81

* Mathematics Department, DePaul University, Chicago IL 60614
** Aiken Computation Lab., Harvard University, Cambridge, MA 02138

This work was supported in part by the National Science Foundation grant NSF-MCS79-21024 and the Office of Naval Research grant (15) N00014-80-C-0647, NSF-MCS-79-21024

THE COMPLEXITY OF PROVABLE PROPERTIES OF FIRST ORDER THEORIES

0. SUMMARY

This paper considers first order quantified and modal theories with the interpretation of function and predicate symbols restricted to fixed r.e. sets of functions F and predicates R. We characterize functions with certain properties (such as totality, monotonicity, unboundedness) provable in these theories. In the case F and R are restricted to a complexity class (such as polynomial time), our results give a characterization of complexity hierarchies (such as the polynomial time hierarchy of Stockmeyer [20]) in terms of the strength of theories whose axioms have restricted quantification. In addition we construct formulas for which provability in these theories implies the collapse of the corresponding complexity hierarchy.

We consider modal theories as well as purely quantified theories. Because modal formulas can encode arbitrary alternations of quantifiers, provability of certain formulas in these modal theories implies the collapse of complexity hierarchies with unbounded alternation. This is applied to the P $\overset{?}{=}$ PSPACE problem.

1. INTRODUCTION

Recent work by Kirby, Paris and Harrington [7] has caused renewed interest in independence results in mathematical logic. Using new methods developed by Paris and Kirby [12], a purely combinatorial statement of arithmetic was shown to be independent of Peano's first order axioms for number theory. In computer science this work together with the observations of Hartmanis and Hopcroft [8] gave rise to the hope that similar methods could be developed to yield interesting independence and consistency results for other naturally arising theories. While this idea has not been completely successful (see O'Donnell [17] for a notable exception), related considerations have yielded a flurry of results relating open problems in computer science and various theories which arise naturally in their study. Significant work in this area can be found in Leivant [15], Lipton and DeMillo [3,4], Lipton [16], Joseph and Young [11], and most recently Paris and Dimitracopoulos [19].

The aim of this paper is to relate the strength of various first order theories to unresolved complexity problems. DeMillo and Lipton have recently considered a first order quantified logic PT whose function and predicate symbols are restricted to polynomial time and whose axioms are all true Σ_2 sentences of this logic. They construct a formula Φ_s for each $s \in NP \cap coNP$ such that $s \in P$ iff $PT \vdash \Phi_s$. Thus $P \overset{?}{=} NP$ can be related to the strength of PT. This paper considers a very general class of first order theories of bounded complexity with a restricted interpretation of the function and predicate symbols. In the main technical theorem we partially characterize the strength of these theories. This result allows us to show that certain functions can be proved within our theory to have particular properties. This work is much in the spirit of Fischer [5] who considered the class of provably total recursive functions.

As applications of the main theorem we have, for each $k \geq 2$ a theory PT_k whose strength is related to the open problem $P \overset{?}{=} \Sigma_{k-1}^{poly}$ of the Stockmeyer polynomial time hierarchy. In addition we have a quantified theory LST whose proof strength we relate to the open problem deterministic linear-space $\overset{?}{=}$ nondeterministic linear-space. Finally, we consider a modal theory MPT and relate it to the $P \overset{?}{=} PSPACE$ problem.

2. PRELIMINARIRES: The Theory $T(Q_k,F,R)$.

Let $N = \{0,1,2,\ldots\}$ be the natural numbers. Let F be a recursively enumerable set of functions on N closed under finite composition and containing all the 0-ary constant functions as well as the function $\ell(x) = |x|$, where $|x|$ denotes the length of the string x. Generally x will be an integer represented as a binary string. We let $f^{(k)}$ designate a k-addic function. We define <u>pred (F)</u> $= \{f \in F \mid \text{range}(f) \subseteq \{0,1\}\}$. Finally let R be an r.e. set of predicates over N.

If Φ is a first order quantified formula of the form $Q_1x_1Q_2x_2\ldots Q_kx_k$ $A(x_1,\ldots,x_k)$ where $A(x_1,\ldots,x_k)$ is a quantifier free formula and the quantifiers $Q_1,\ldots,Q_k \in \{\forall,\exists\}$ alternate k-1 times, then we say Φ is in Σ_k-*form* if $Q_1 = \exists$ and in Π_k-*form* if $Q_1 = \forall$. A quantifier free formula is said to be in both Σ_0 *form* and Π_0 *form*. We define Φ to be in Δ_k if there are formulas ψ_1,ψ_2 in Σ_k and Π_k form respectively such that $N \models \Phi \leftrightarrow \psi_1 \leftrightarrow \psi_2$.

We now define a theory $T(Q_k,F,R)$ where $Q_k \in \{\Sigma_k,\Pi_k\}$ and F and R are as above. The idea is that $T(Q_k,F,R)$ is the theory whose axioms are all true Q_k formulas which have Skolem functions that are Σ_{k-2} definable over F and R. To make this notion precise we give the following definitions. The language for our theory consists of symbols for all functions in F and predicates in R together with the usual connectives and quantifiers of first order logic. We call a function $g\colon N \to N$ Σ_m-*definable* if there is a Σ_m formula of our language which defines the function g. Note: To simplify notation we will often write a formula as containing such Σ_m definable functions g. Such formulas could be precisely written by replacing all occurrences of such functions by the Σ_m formula which defines them. Now let $\underline{C_m}$ be the class of all Σ_m definable functions.

Given a true (in the standard model) sentence $\Phi = \forall x_1 \exists x_2 \ldots Q x_k\ A(x_1 \ldots x_k)$ in Π_k form, we say the C_m *contains Skolem functions* for Φ if for some $g^1, g^2, \ldots$ in C_m we have $\forall x_1 \forall x_3 \ldots\ A(x_1, g^1(x_1), x_3, g^2(x_1, x_3), \ldots)$. We now let $T(\Sigma_k, F, R)$ $[T(\Pi_k, F, R)]$ be the collection of all $\Sigma_k [\Pi_k]$ formulas with Skolem functions in $C_{k-2} [C_{k-1}]$. The theory $T(\Delta_k, F, R)$ is defined analogously. Also let $T(Q_k, F) = T(Q_k, F, \mathrm{pred}(f))$. We say that $T(Q_k, F)$ is a *complexity theory over* F if F is defined by a recursive bound on a complexity measure (see Blum [1]).

For example DeMillo and Lipton [3,4] consider:

(i) The "polynomial time" theory $PT = T(\Sigma_2, \mathrm{poly})$ where poly is the class of polynomial time computable functions. The equality is essentially proved in [2].

(ii) The "poly-time predicate, arithmetic and exponential function" theory $ET = T(\Pi_1, \mathrm{arith}, \mathrm{pred}(\mathrm{poly}))$ where arith consists of function built from addition, multiplication and exponentiation. In [4] DeMillo and Lipton show that ET + "P = NP" is a consistent theorem. It is interesting to note that their proof is actually sufficient to show that ET is consistent with $P = \Sigma_k^{\mathrm{poly}}$ and then by compactness $P = \bigcup_{k \geq o} \Sigma_k^{\mathrm{poly}}$ is consistent with ET.

In our own applications we shall consider the "polynomial-time hierarchy theory" $PT_k = T(\Sigma_k, \mathrm{poly})$. We may also allow F to correspond to other complexity classes such as the linear-space functions. Here we consider LST = $T(\Sigma_2, \text{linear-space})$. In the last sections we consider a modal theory MPT whose properties depend on PSPACE even though F = poly time for MPT.

3. "HERBRAND" THEOREMS FOR $T(Q_k,F)$

In this section we give model theoretic proof of Herbrand expansion theorems for the theories $T(\Sigma_{k+2},F)$ and $T(\Pi_{k+2},F)$. These theorems will be the main technical tool used in later sections where we give lower bounds for the complexity of provable properties in $T(\Sigma_{k+2},F)$ and $T(\Pi_{k+2},F)$.

We frequently write a formula in "standard form" where in the matrix of the formula the universally quantified variables all preceed the existentially quantified variable. More precisely we define a Π_j sentence Φ to be in k-*standard form* if $\Phi = Q_1x_1Q_2x_2 \ldots A(\bar{x}^u,\bar{x}^e)$ where $Q_1 = \forall$, $A \in \Pi_k$, and the variables of A are partitioned into universal variables $\bar{x}^u$ and existential variables $\bar{x}^e$ which appear in the same order in which they appear in A. Note that if $j-k$ is odd the A is actually in Π_{k-1} rather than just in Π_k.

For any Π_j sentence Φ in k-standard form and any $C_0 \subseteq C_{k-2}$, C_0 finite, define

$$\Phi_{C_0} = \forall \bar{x}^u \bigvee_{g^1,\ldots,g^u \in C_0} A(\bar{x}^u, g^1(x_1),\ldots,g^{(u)}(\bar{x}^u)) \quad .$$

Recall that C_{k-2} is the collection of all Σ_{k-2} definable functions of one of our theories. So the g's which appear in the above formula represent Σ_{k-2} formulas of our logic which define functions.

Before stating the main technical theorem we need the following proposition:

DEFINITION. *Given two structures* M_1 *and* M_2 *we say* M_2 *is a* Σ_k-substructure *of* M_1 *if*

(1) M_2 *is a substructure of* M_1.

(2) *For any formula* $\Phi \in \Sigma_k$, *if* $M_1 \models \Phi$ *then* $M_2 \models \Phi$.

PROPOSITION. *If* $M_1 \models T(\Sigma_{k+2},F)$ *and* M_2 *is a* Σ_k*-substructure of* M_1 *then* $M_2 \models T(\Sigma_{k+2},F)$.

Proof. Let $\exists x\forall y\Phi(x_1 y)$ be a Σ_{k+2} formula in $T(\Sigma_{k+2},F)$, where $\Phi(x,y)$ is in Σ_k. Then $N \models \exists x\forall y\Phi(x,y)$ so for some $n_0 \in N$, $N \models \forall y\Phi(n_0 y)$. As $M_1 \models T(\Sigma_{k+2},F)$ we have $M_1 \models \forall y\Phi(n_0,y)$. Now M_2 is a Σ_k-substructure of M_2 and so any Π_{k+1} formula true in M_1 is true in M_2 as well in particular $M_2 \models \forall y\Phi(n_0,y)$ and so $M_2 \models \exists x\forall y\Phi(x,y)$.

THEOREM 1A. *Let* $T = T(\Sigma_{k+2},F)$ *and* Φ *be a* $\Pi_j (j \geq k)$ *formula in* k-*standard form. Then* $T \vdash \Phi$ *implies that for some finite* $C_0 \subseteq C_k$, $T \vdash \Phi_{C_0}$.

Proof. Suppose $T \vdash \Phi$ but $T \nvdash \Phi_{C_0}$ for any finite $C_0 \subseteq C_k$. Let T^* be the theory derived from T by adding distinct constant symbols $c_1, c_2, \ldots c_u$ to our language and adding axioms $\sim A(\bar{c}, g^1(x_1), g^2(x_1,x_3)\ldots)$, for every $g^1, g^2, \ldots$ in C_k. Observe that T^* is consistent. (Otherwise, by compactness, there is a finite $C_0 \subseteq C_k$ such that $T \vdash \Phi_{C_0}$, contradicting our assumption.) So T^* has a model M. Let $M_{\bar{c}}$ be the submodel of M generated by applying the functions of C_k to the constants which interpret $c_1,\ldots,c_u$ in M. Then $M_{\bar{c}}$ is a Σ_k-substructure of M. Now let Φ' be the formula $\exists \bar{x}^e A(\bar{c},\bar{x}^e)$. Then as $M \models T$, by the above proposition we have $M_{\bar{c}} \models \Phi'$. But by the definition of T^* and the construction of $M_{\bar{c}}$ we have $M_{\bar{c}} \models \neg\Phi'$, a contradiction which proves the theorem.

Similarly we can show,

THEOREM 1B. *If* $T = T(\Pi_{k+1},F)$ *and* Φ *is a* Π_j *formula in* k-*standard form then* $T \vdash \Phi$ *implies* $T \vdash \Phi_{C_0}$ *for some finite* $C_0 \subseteq C_k$.

4. PROVABLE PROPERTIES OF FUNCTIONS

For $\bar{x} = x_1,\ldots,x_m$ the formula $\Phi(\bar{x})$ is x-*bounded* if each quantifier Q of Φ has the form $Qx(|x| \le \max(|x_1|,\ldots,|x_m|))$. We will usually write this as $Qx \le^* \max(\bar{x})$. For any formula $\psi(\bar{x})$, let $\hat{\psi}$ be the function such that $\forall\bar{x} \in N^m$, $\hat{\psi}(\bar{x}) = 1$ if $\psi(\bar{x})$ holds and $\hat{\psi}(\bar{x}) = 0$ otherwise. Define $Q_k^F = \{\hat{\psi} | \psi(\bar{x})$ is an x-bounded formula in the logic with symbols for elements of F which are in Q_k-form with m free variables$\}$. Let $f;N \to \{0,1\}$ *denote* $S \subseteq N$ if $S = f^{-1}[1]$. In the case that F = polynomial-time, Σ_k^F, Π_k^F, Δ_k^F denote the complexity classes of the polynomial-time hierarchy of Stockmeyer [20].

We say a function $f\colon N^m \to N$ is *defined by a formula* Θ if $\forall x,y$ $f(\bar{x}) = y$ iff $\Theta(\bar{x},y)$. Let $B = \{f | f(\bar{x})$ is a function $N \to \{0,1\}$ defined by x-bounded formula $\theta(\bar{x},y)$ of the logic$\}$.

DEFINITION. $f\colon N^m \to N$ *is* provably total in a theory T *if* f *is defined by a formula* $\Theta(\bar{x},y)$ *and* $T \vdash \forall\bar{x}\exists y\, \Theta(\bar{x},y)$.

THEOREM 2A. *For each* $k > 1$, *let* $T = T(\Sigma_{k+2},F)$. *Then* $\{f \in \Delta_k^F | f$ is total$\} \subseteq \{f \in B | f$ is provably total in $T\} \subseteq \Pi_k^F$.

<u>Proof</u>. (a) Let $f \in \Delta_k^F$ be total. Then there exists x-bounded formulas ψ_1,ψ_2 in Σ_k-form such that $f(\bar{x}) = 1$ iff $\psi_1(\bar{x})$ iff $\sim\psi_2(\bar{x})$. Let $\Theta(\bar{x},y) = (y=1 \wedge \psi_1(\bar{x})) \vee (y=0 \wedge \psi_2(\bar{x}))$. f is defined by $\Theta(\bar{x},y)$. Then $\forall\bar{x}\exists y\Theta(\bar{x},y)$ is a true Π_{k+1} formula and hence an axiom of T (since f is its Skolem function). So f is provably total in T.

(b) Let $f\colon N^m \to N$ where $f \in B$ and f is provably total in T. Then f is defined by an x-bounded formula $\Theta(x,y)$ which can be represented as

$$\Theta(x,y) = Q_1 z_1 \le^* \max(\bar{x}),\ldots,Q_m z_m \le^* \max(\bar{x}) A(\bar{x},\bar{z}^u,y,\bar{z}^e)$$

where $\bar{z}^e$ are the existentially quantified variables *among* $z_1,\ldots,z_m$ and $\bar{z}^u$ the universally quantified variables. Let Φ be the formula $\forall x\exists y\Theta(x,y)$. So we have $T\vdash\Phi$ and by Theorem 1A, for some finite $C_0 \subseteq C_k$, $T\vdash\Phi_{C_0}$. From the definition of Θ we see that

$$\Phi_{C_0} = \forall\bar{x}\,\forall\bar{z}^u \le^* \max(\bar{x}) \bigvee_{g^1,\ldots g^{m+1}\in C_0} A(\bar{x},\bar{z}^u,g^1(\bar{x}),\ldots,g^{m+1}(\bar{x},\bar{z}^u)).$$

Let $\Theta_{C_0}(x,y)$ be the formula

$$\forall\bar{z}^u \le^* \max(\bar{x}) \bigvee_{g^1,\ldots g^{m+1}\in C_0} A(\bar{x},\bar{z}^u,y,g^2(\bar{x},z_1),\ldots,g^{m+1}(\bar{x},\bar{z}^u)).$$

$T\vdash \forall\bar{x}\Theta_{C_0}(\bar{x},y)$ and Θ_{C_0} is an x-bounded Π_k formula which holds in N iff $f(\bar{x}) = y$. So $\hat{\Theta}(\bar{x},y) = 1$ if $f(\bar{x}) = y$ and is 0 otherwise and we have $\Theta_{C_0} \in \Pi_k^F$.

Note: This same theorem can be shown for the theory $T(\Pi_{k+1},F)$ rather than $T(\Sigma_{k+2},F)$.

The lower bounds of the above theorems can be shown as well for many other properties of functions. For example they can be shown for functions which are surjective $\forall y\exists\bar{x}\ f(\bar{x}) = y$ and for functions which are unbounded, $\forall y\exists\bar{x}\ f(\bar{x}) > y$. In general, any class of functions definable by a Π_2 property are such that any Δ_k^F members of the class are provably in the class .

Let Σ_* denote unrestricted quantification and let $\Sigma_*^F = \bigcup_k \Sigma_k^F$. As an immediate consequence of Theorem 2A we have

COROLLARY: 2B. $\Sigma_*^F = \{f \in B\ f$ is provable total in $T(\Sigma_*,F)\}$.

A similar corollary can be proved for any Π_2 definable property of functions.

In the case F = poly, the (total) polynomial-time computable functions, we have $P \neq \Sigma_k^{poly}$ iff there is a total function $f \in B \cap \Sigma_k^{poly}$ which isn't provably total in $PT_0 = T(\Sigma_2, poly)$. It should be noted, however, that we cannot characterize the $P \overset{?}{=} PSPACE$ problem by a similar technique in the theory $PT_* = T(\Sigma_*, poly)$ since each element of Σ_*^{poly} corresponds to a quantified formula with some *bounded* alternation of quantifiers. We will use a modal theory in Section 6 to characterize this problem since formulas in modal logic can express unbounded alternation.

5. COMPLEXITY CLASSES AND HIERARCHIES OF PROVABILITY

In this section we construct formulas for which provability in our theories implies collapse of the corresponding complexity classes.

THEOREM 3A. *For each* $k \geq 0$, $j \geq k+1$ *and* $f \in \Delta_j^F$, *there is a formula* Φ *such that* $f \in D$ *iff* $T \vdash \Phi$, *where* $T = T(\Sigma_{k+2}, F)$ *and*

$$D = \begin{cases} \Delta_1^F & \textit{if } k = 0 \textit{ and } j > 1. \\ \Delta_k^F & \textit{otherwise.} \end{cases}$$

<u>Proof</u>. Since $f \in \Delta_j^F$ there must be x-bounded formulas ψ_1 and ψ_2 in Π_j-form such that $f(\bar{x}) = 1$ iff $\psi_1(\bar{x})$ iff $\sim\psi_2(\bar{x})$. For $i = 1,2$ let $\psi_i(\bar{x}) = Q_1 z_1 \leq^* \max(\bar{x}), \ldots, Q_m z_m \leq^* \max(\bar{x}) G_i(\bar{x}, \bar{z}^u, \bar{z}^e)$, where G_i is an x-bounded Π_k formula and $Q_1 = \forall$. Define Φ by $\forall \bar{x} \psi_1(\bar{x}) \vee \psi_2(\bar{x})$. So Φ may be written as $\forall \bar{x} Q_1 z_1 \leq^* \max(\bar{x}), \ldots, Q_m z_m \leq^* \max(\bar{x}) A(\bar{x}, \bar{z}^u, \bar{z}^e)$ with A an x-bounded formula in Π_k-form.

(a) Suppose $f \in D$. Then $A(\bar{x}, \bar{z}^u, \bar{z}^e) = A(\bar{x}, \bar{z}^{u'})$ where $\bar{z}^{u'}$ are the universally quantified variables of $\bar{z}$ preceeding the first existential variable of $\bar{z}$. So $\Phi = \forall\bar{x}\forall\bar{z}^{u'} A(\bar{x}, \bar{z}^{u'})$ is a Π_k formula (Π_1 if $k = 0$) which is true in N and hence an axiom of T.

(b) Suppose $T \vdash \Phi$. Then by Theorem 1A, for some finite $C_0 \subseteq C_k$, $T \vdash \forall\bar{x}(\psi_{1,C_0}(\bar{x}) \vee \psi_{2,C_0}(\bar{x}))$ where for $i = 1,2$ we have $\psi_{i,C_0}(\bar{x}) =$

$$\forall z_1 \leq^* \max(\bar{x}), \ldots, z_u \leq^* \max(\bar{x}) \bigvee_{g^m \ldots g^{m+u} \in C_0} G_i(\bar{x}, \bar{z}^u, g^m(\bar{x}), g^{m+1}(\bar{x}, z_1), \ldots, g^{m+u}(\bar{x}, \bar{z}^u)).$$

We then have $f(\bar{x}) = 1$ iff $\psi_{1,C_0}(\bar{x})$ iff $\sim\psi_{2,C_0}(\bar{x})$. Let $\Phi(\bar{x}) = \sim\psi_{2,C_0}(\bar{x})$. If $k = 0$ and $j > 1$ then $\hat{\psi}_{1,C_0} \in \Pi_1^F$ and $\hat{\Phi} \in \Sigma_1^F$ so $f \in \Delta_1^F$. Otherwise, if $k > 0$, we have $\hat{\psi}_{1,C_0} \in \Pi_k^F$ and $\hat{\Phi} \in \Sigma_k^F$ so $f \in \Delta_k^F$. In either case $f \in D$.

Note: Theorem 3A generalizes the main result of DeMillo-Lipton [2].

Let $f\colon N^m \to N^n$ and $L_1 \subseteq N^m$, $L_2 \subseteq N^n$. We call f an F-*reduction* from L_1 to L_2 if $f \in F$ and $x \in L_1$ iff $f(x) \in L_2$. L is F-*complete in* D if $L \in D$ and for each $L' \in D$ there is an F-reduction from L' to L.

COROLLARY: 3B. *Let* D *be as in Theorem* 3A. *If* Σ_{j-1}^F *has an element* F-*complete in* D *then there is a formula* Φ *such that* $\Sigma_{j-1}^F \subseteq D \leftrightarrow T(\Sigma_{k+2}, F) \vdash \Phi$

When F = poly there are a number of applications of the above results to the polynomial time hierarchy of Stockmeyer. Let $PT_k = T(\Sigma_{k+2}, \text{poly})$. Then since each $\Sigma_{j-1}^{\text{poly}}$ has a poly-complete element, there is a formula Φ such that $\Sigma_{j-1}^{\text{poly}} \subseteq \Delta_k^{\text{poly}}$ if $PT_k \vdash \Phi$ for $k > 0$ or $j = 1$, and there is a formula Φ' such that $\Sigma_{j-1}^{\text{poly}} \subseteq \Delta_1^{\text{poly}}$ iff $PT_0 \vdash \Phi'$.

There is a similar application for the case F = poly-space to the hierarchy of k-bounded alternation machines with polynomial space. (See [2].)

6. COMPLEXITY OF PROVABLE PROPERTIES OF FIRST-ORDER MODAL THEORY

We note in this final section that our results extend to a first-order theory with modal operator $\Box$ (with the Kripke semantics of the propositional modal system K considered in [10] and [13]) and the usual first-order quantifiers $\forall$ and $\exists$. Let $MT(Q,F)$ be the first-order modal theory defined as in the previously defined theories $T(Q,F)$ but allowing our formulas to contain the modal operator $\Box$ and our theory to contain the modal axioms:

rule of necessity:

$$\vdash \Box A \text{ if } \vdash A$$

and *modal induction* K:

$$\vdash \Box (A \supset B) \supset (\Box A \supset \Box B).$$

The proof of Theorem 1A implies the following (somewhat more restricted) "Herbrand" expansion result for the theory $T = MT(\Sigma_*,F)$.

COROLLARY: 1A. *If* Φ *is a formula of the form* $\forall\bar{x}\exists\bar{y}\psi(\bar{x},\bar{y})$ *and if* $T\vdash\Phi$ *then for some finite* $C_0 \subseteq C_*$,

$$T\vdash\forall\bar{x} \bigvee_{g^1\ldots g^m \in C_0} \psi(x,g^1(x_1),\ldots,g^m(\bar{x})),$$

where $C_* = \bigcup_k C_k$.

Likewise, the proof of Theorem 2A implies a somewhat weaker result for $MT(\Sigma_*,F)$. Let $M^F = \{\hat{\psi}|\psi(x)$ is an x-bounded modal formula with symbols for elements of $F\}$ and let $MB = \{f \mid f(\bar{x})$ is a function $N \rightarrow \{0,1\}$ defined by an $\bar{x}$-bounded modal formula$\}$.

COR. 2A. $\{f \in M^F \mid f$ is total$\} = \{f \in MB \mid f$ is provably total in $MT(\Sigma_*, F)\}$.

There are some interesting applications to complexity theory in the case F = poly, the total polynomial-time computable functions. Stockmeyer [20] has shown that the validity problem for the quantified boolean logic QBF is PSPACE-complete, and Ladner [14] has shown the validity problem for the propositional modal system K is PSPACE-complete. The propositional modal system K augmented with quantification of boolean variables also has a PSPACE-complete validity problem. This implies that MB is the polynomial space computable 0,1 functions. Thus $P \neq$ PSPACE if there is an $f \in B$, $f \notin$ polynomial-time such that f is not provably total in the theory $MT(\Sigma_*,$poly$)$.

BIBLIOGRAPHY

1. M. Blum, "A machine independent theory of complexity of recursive function," JACM 14(2), April 1967.

2. A. Chandra, D. Kozen, L. Stockmeyer, "Alternation," IBM Tech. Report, 1978.

3. R.A. DeMillo and R.J. Lipton, "Some connections between mathematical logic and complexity theory," Proc. of the 11th Symposium on the Theory of Computation, 1979.

4. R.A. DeMillo and R.J. Lipton, "The consistency of "P = NP" and related problems wity fragments of number theory," 12 Symp. on Theory of Computing, April 1980.

5. P.C. Fischer, "Theory of provably recursive functions," TAMS 117(5), 1965.

6. D. Gordon, "Complexity classes of provably recursive functions," J. Computer and Systems Sciences, 18(3), 1979.

7. L. Harrington and J. Paris, "A mathematical incompleteness in Peano arithmetic," in *Handbook of Mathematical Logic,* Barwise editor, North-Holland, 1978.

8. J. Hartmanis and J.E. Hopcroft, "Independence results in computer science," SIGACT News 8(4), 1976.

9. J. Hartmanis, "Relation between diagonalization, proof systems and complexity gaps," Proc. of the 9th Symposium on the Theory of Computation, 1977.

10. G.E. Hughes and M.J. Cresswell, "An Introduction to Modal Logic," Methuen, London, 1968.

11. D. Joseph and P. Young, "Independence results in computer science," 12th Symp. on Theory of Computing, April 1980.

12. L. Kirby and J. Paris, "Initial segments of models of Peano's axioms," Proc. Conf. Set Theory and Hierarchy Theory V, Springer-Verlag Lecture Notes #619, 1976.

13. S.A. Kripke, "Semantical analysis of modal logic, I. Normal modal propositional calculi," Z. Math. Logik Grundlagen Math., 9 (1963), pp. 67-96.

14. R.E. Ladner, "The computational complexity of provability in systems of modal logic," SIAM J. Computing, 1977.

15. D. Leivant, "On easily finite sets and a statement of R. Lipton," to appear.

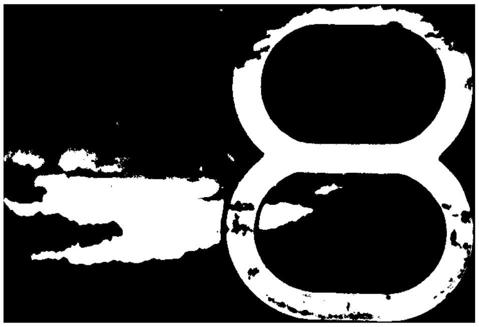
16. R.J. Lipton, "Model theoretic aspects of complexity theory," Proc. of the 19th FOCS conference, 1978.

17. M. O'Donnell, "A programming language theorem which is independent of Peano arithmetic," Proc. of the 11th Symposium on the Theory of Computation, 1979.

18. J.B. Paris, "Some independence results for Peano arithmetic," JSL 43, 1978.

19. J.B. Paris and C. Dimitracopoulos, "Truth definitions for Δ_0 formulas,"

20. L.J. Stockmeyer, "The polynomial-time hierarchy," IBM Tech. Report, 1975.



8